GT GreenbergTraurig

Alert | Export Controls & Economic Sanctions

September 2022

New Executive Order Identifies National Security Risks for CFIUS to Consider When Assessing Foreign Investment in US Businesses

Go-To Guide:

- First-of-its-kind Executive Order articulates specific industries and areas of national security scrutiny on inbound investment into the United States.
- Focus on supply chain security, emerging technologies, cybersecurity and sensitive data of U.S. persons.
- Does not change the current regulations on mandatory declaration to CFIUS of certain investment transactions.
- Puts foreign investors and U.S. targets of investment on notice that the identified areas will face scrutiny, even potentially in "non-notified" transactions that could be reviewed by CFIUS (and/or ordered to be unwound) post-closing.

On Sept. 15, 2022, President Biden issued an Executive Order (EO) providing formal direction to the Committee on Foreign Investment in the United States (CFIUS) concerning additional risks to be considered when examining foreign investments. Although the EO does not expand CFIUS jurisdiction or alter the existing U.S. foreign direct investment review process, it does represent the first presidential

directive of its kind and signals the U.S. government's scrutiny of foreign investments is likely to continue unabated.

National Security Review Factors Set Forth in the EO

The EO ("Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States") directs CFIUS to consider five specific risk categories listed below in connection with foreign investment transactions in the United States. Notably, the EO is not an exhaustive list of factors that CFIUS must take into account in its review, but instead emphasizes the U.S. government's particular interest in the five enumerated risks (among other national-security-related risks and considerations). The EO also reaffirms provisions of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) that highlight national security risks arising from foreign investments involving "a country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect United States leadership in areas related to national security." While neither FIRRMA nor the EO explicitly identifies any country presenting elevated national security risks to the United States, it does direct CFIUS to consider the direct or indirect involvement of "foreign adversaries and other countries of special concern" and foreign investor's "relevant third-party ties" to foreign governments or foreign persons when analyzing the threat of a transaction. These criteria are not new per se for CFIUS, but for the first time are expressly articulated in a Presidential EO. It will be particularly important going forward for investors and targets of investment to consider not only the existing CFIUS regulations regarding mandatory declarations to CFIUS in certain investment transactions but also, in the broader scope of transactions that are ripe for voluntary CFIUS notification, that the articulation of these key areas may tip the scales toward voluntary notification in some instances.

The EO does not limit CFIUS' authority to interpret U.S. national security interests broadly in the context of foreign acquisitions or investments (known as "covered transactions"), and to a large extent the five articulated factors simply confirm areas already known to be of concern to CFIUS. For example, national security factors 1 and 2 are already described in Section 721 of the Defense Production Act (DPA), CFIUS' authorizing statute.

1. **Protection of Supply Chain Resilience and Security.** The EO directs CFIUS to consider "the covered transaction's effect on supply chain resilience and security, both within and outside of the defense industrial base, in manufacturing capabilities, services, critical mineral resources, or technologies that are fundamental to national security, including: microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy (such as battery storage and hydrogen), climate adaptation technologies, critical materials (such as lithium and rare earth elements), elements of the agriculture industrial base that have implications for food security, and any other sectors identified in section 3(b) or section 4(a) of Executive Order 14017 of February 24, 2021 (America's Supply Chains)."

2. **Risk to U.S. Technological Leadership.** The EO directs CFIUS to consider whether a covered transaction will impact technologies that are vital to U.S. technological leadership, including but not limited to manufacturing capabilities, services, critical mineral resources, microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies. Additionally, CFIUS is also directed to consider whether a covered transaction could result in future technological advancements that could undermine U.S. national security.

3. **Risk of Incremental Industry Investment Trends.** The EO requires CFIUS to evaluate the potential risks arising from multiple acquisitions or investments in a single sector or in related manufacturing capabilities, services, or critical mineral resources. Investments that appear to be minor or unsuspicious viewed in isolation could in fact be part of a broader scheme culminating in the transfer of sensitive technology in key U.S. industries, undermining U.S. national security.

4. **Risk to Cybersecurity.** The EO directs CFIUS to consider whether the foreign investor (including its relevant third-party ties) may as a result of the investment directly or indirectly obtain the ability to harm U.S. cybersecurity.

5. **Risk to Sensitive Data.** The EO directs CFIUS to consider whether a covered transaction involves the transfer of U.S. persons' sensitive data to a foreign person. Additionally, the EO directs CFIUS to assess whether a covered transaction involves investment into or acquisition of a U.S. business that has access to or that stores:

    a. U.S. persons' sensitive data, including health, digital identity, or other biological data and any data that could be identifiable or de-anonymized, that could potentially be exploited to reveal an individual's identity in a manner that undermines U.S. national security; or

    b. U.S. sub-population data that could be used by a foreign person to target persons in the United States in a manner that threatens national security.

Key Takeaways

Despite not altering the scope of CFIUS authority, the EO demonstrates the president's endorsement of inbound investment review and articulates to practitioners and members of the investment community five key areas of particular national security sensitivity. The considerations are largely in line with the areas of focus CFIUS has prioritized historically and in recent years, and while the EO does not specifically grant CFIUS new authority, the EO could fuel CFIUS' appetite for review of future inbound investments. For example, the EO marks the first time the U.S. government has focused on the risk of foreign investment in the advanced clean energy sector in the United States. Parties to an investment or M&A transaction should assess first whether a transaction is subject to mandatory declaration under existing CFIUS regulations, and even if not, then consider the likelihood of a CFIUS review and the potential benefits to file a voluntary notice or declaration. The analysis of whether a CFIUS filing is legally required or advisable can be complex, and parties to a foreign investment transaction in the United States should begin this process as early in the transaction as possible.

Click here to learn about Greenberg Traurig's Export Controls & Economic Sanctions Practice.

Authors

This GT Alert was prepared by:

- Kara M. Bombach | +1 202.533.2334 | bombachk@gtlaw.com
- Cyril T. Brennan | +1 202.533.2342 | brennanct@gtlaw.com
- Sonali Dohale | +1 202.533.2381 | dohales@gtlaw.com
- Francisco J. Vélez ǂ | +1 202.533.2331 | velezf@gtlaw.com

‡ Admitted to practice in Florida. Practice in District of Columbia limited to federal courts and agencies.

Albany. Amsterdam. Atlanta. Austin. Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Long Island. Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.